JAP: KTF

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- X
IN THE MATTER OF AN APPLICATION FOR A SEARCH WARRANT FOR:

THE PREMISES KNOWN AND DESCRIBED AS 981 PARK PLACE, APT 2C, BROOKLYN, NY 11213
- X

16M 812

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

UNDER SEAL

EASTERN DISTRICT OF NEW YORK, SS:

BRIAN URIBE, being duly sworn, deposes and states that he is a Special Agent with Homeland Security Investigations, duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that, located in THE PREMISES KNOWN AND DESCRIBED AS 981 PARK PLACE, APT 2C, BROOKLYN, NY 11213 (the "PREMISES") further described in Attachment A, there are the items described in Attachment B, which constitute evidence, fruits, and instrumentalities of the possession, access with intent to view, transportation, receipt, distribution, and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A.

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I am a Special Agent with Homeland Security Investigations. I have been employed by Homeland Security Investigations since 2001, and am currently assigned to the Child Exploitation Investigation Unit ("CEIU"). I have been assigned to investigate violations of

[1] Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

criminal law relating to the sexual exploitation of children. I have gained expertise in this area through training in classes and daily work related to these types of investigations. As a result of my training and experience, I am familiar with the techniques and methods of operations used by individuals involved in criminal activity to conceal their activities from detection by law enforcement officers. As part of my responsibilities, I have been involved in the investigation of several child pornography cases and have reviewed photographs depicting children (under eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in this investigation, and (b) reports made to me by other law enforcement authorities.

3. Homeland Security Investigations is investigating the possession, access with intent to view, transportation, receipt, distribution, and reproduction of sexually explicit material relating to children in violation of Title 18, United States Code, Sections 2252 and 2252A.

I. DEFINITIONS

4. For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct," and "visual depiction" are defined as set forth in Title 18, United States Code, Section 2256.

b. The term "child pornography" is defined in Title 18, United States Code, Section

2256(8) in pertinent part as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. . . ."[2]

c. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data-processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.

d. The term "IP Address" or "Internet Protocol Address" means a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. The term "Internet" refers to a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. The term "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

II. BACKGROUND

A. PEER TO PEER FILESHARING

5. Peer to peer file sharing ("P2P") is a method of communication available to Internet users through the use of special software. Computers linked together through the

---

[2] *See also Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

Internet using this software form a network that allows for the sharing of digital files between users on that network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer.

6. The latest evolution of P2P software is a program that allows a user to set up his or her individual private P2P network of contacts. File sharing through this new and publicly available P2P file sharing program is limited only to other users who have been added to a private list of "friends." A new user is added to a list of friends by request. Acceptance of a friend request will allow that new user to download files from the user who sent the friend request. The new user can then browse the list of files that the other user has made available to download, select desired files from this list, and download the selected files. The downloading of a file occurs through a direct connection between the computer requesting the file and the computer containing the file.

7. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time.

8. A P2P file transfer is assisted by reference to an IP address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

9. Third-party software ("Network Monitoring Program" or "Investigative Software") is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

10. In order for the P2P networks to accomplish the reassembly of files described above, files being shared on the P2P network are processed through the client software and, a hashed algorithm value ("hash value") is computed for each file being shared, which uniquely identifies it on the network. A file processed by this hash algorithm operation results in the creating of an associated hash value often referred to as a digital signature, akin to a fingerprint. P2P software uses these hash values to determine whether files hosted on different computers with different names are, in fact, the same file.

11. One investigative method employed in this investigation involves the use of Investigative Software ("IS") that is used in P2P file sharing investigations to directly download files of child pornography from P2P network users. The IS is designed to "direct connect" to one IP address and browse or download from one specific P2P network user at a time. The IS is P2P file-sharing software similar to the other file-sharing software used on P2P networks which are free and available to the public.

B. THE INVESTIGATION

12. In June 2016, an HSI agent signed into a P2P network using IS computer software. The IS located a computer using the IP Address 24.228.93.157 ("IP Address") that was using the P2P network to make available certain hash values and files with file names that contained certain words generally known to be associated with child pornography images and

videos, and which are known by law enforcement to match suspected child pornography hash values.

13. On June 13, 2016, the IS "direct connected" to the IP Address and displayed numerous files being hosted by the user of said IP address. Using the IS and P2P networks, the HSI agent downloaded numerous files from the computer at the IP Address to include the following, which are available for the Court's review:

a. A wmv video file "52.wmv", approximately 1 min long, depicting a young prepubescent female on her hands and knees being penetrated by an adult male with his erect penis, from behind. Hash Value: SHA1=DE4A7DDE2E5ADF7D183EDBF9D233D8B0DCB61CC1

b. An avi file named "9Yo Arab Pedo Girl Fucked By Dad.avi", approximately 1 min long and 1 second, depicting a nude prepubescent female wearing sunglasses while standing in a shower. The scene switches to show the same female lying on a bed with towel covering her. The towel is pulled off, exposing her nude body, while an adult male penis is seen rubbing against her vagina. The scene again switches, depicting the same female sitting on an adult male as he appears to have intercourse with her. The scene again switches to depict an adult male rubbing his penis against her vagina, with the female eventually masturbating the male penis. Hash Value: SHA1=E519ED6A3F9CCDE60642AD6B151ABD6B94597747

c. An mpeg file named "(Children-Sf-1Man) Pthc- Norma Latinos Girl 12 Yo Fuck and Suck.mpg", approximately 4min and 43 seconds long, depicting a young

prepubescent female child performing oral sex on an adult male. Approximately 54 seconds into the video, she gets on top of the male as he rubs his penis against the female's vagina until he ejaculates. At approximately 4 minutes, 16 seconds the video depicts numerous images of the female laying on a bed spreading her legs exposing her genitals. Hash Value: SHA1=A34FB0EC6B350217418981FD0FA58B75D90A842A

d. An avi file named "!!!New!!! (Pthc) Nina 2 (7Yo Bj) And 7Yo Suck 2.avi", approximately 2 minutes, 13 seconds long, depicting a young prepubescent female laying naked on a bed. At approximately 20 seconds, an adult hand comes into the frame and repositions the female. At approximately 57 seconds, and adult male penis is inserted into her mouth and the male masturbates into her mouth. Hash Value: SHA1=1EBAF2EBC73211E66421092F86864C39D6DD9241

14. Records from public internet searches and Optimum Online revealed that the account using the IP during June of 2016 is registered to Aaron Robinson at 981 PARK PLACE, APT 2C, BROOKLYN, NY 11213, the PREMISES. Optimum Online records as of June 2016 further revealed that said account is currently active.

15. A search of public records and law enforcement databases revealed that Aaron Robinson currently resides at the PREMISES.

III. THE PREMISES

13. 16. The PREMISES is located within a 6-story brick apartment building at 981 PARK PLACE, APT 2C, BROOKLYN, NY 11213. The front entrance is clearly

marked as being address number "981-985" and is locked with a metal door that requires a key for entry. On July 27, 2016, I entered the building and located apartment 2C, which is located on the 2nd floor, to the left of exiting the elevator. The door to apartment 2C is described as being a dark-green metal door with a doorbell button with a label on it that lists it as "2C". Checks on the mailbox for 2C shows it clearly labeled with the name "Robinson." While it appears based on the database checks and surveillance that Robinson resides alone, the investigation has not concluded at this time whether other individuals reside in the PREMISES. Surveillance and online activity monitoring further confirm that Robinson continues to reside at the PREMISES.

IV. CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

18. Based on my training, and experience, and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

19. I know that collectors of child pornography typically retain their materials and related information for many years.

20. I also know that collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

21. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

22. Based on my experience, I know that persons who collect and distribute child pornography frequently collect sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides, and/or drawings or other visual media that they use for their own sexual arousal and gratification. Further, based on my training, knowledge, experience, and discussions with other law enforcement officers, I understand that, in the course of executing a search warrant for the possession, transportation, receipt, distribution, or reproduction of sexually explicit material related to children, officers on numerous occasions have recovered evidence related to the production of child pornography and/or child exploitation.

V. TECHNICAL BACKGROUND

23. As described above and in Attachment B, this application seeks permission to search for documents constituting evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A that might be found on the PREMISES in whatever form they are found. One form in which the documents might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

24. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from the use of an operating system or application, file

system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on the evidence that a computer connected to a P2P network through an IP address registered at the PREMISES, there is reason to believe that there is a computer currently located on the PREMISES.

25. As further described in Attachment B, this application seeks permission to locate not only electronic computer files that might serve as direct evidence of the crimes described on the warrant, but also electronic "attribution" evidence that establishes how the computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer or storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage

medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, Internet search histories, configuration files, user profiles, email, email address books, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how the computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on a computer is

evidence may depend on the context provided by other information stored on the computer and the application of knowledge about how a computer functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, it is sometimes necessary to establish that a particular item is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

26. In most cases, a thorough search for information that might be stored on computers and storage media often requires agents to seize such electronic devices and later review the media consistent with the warrant. This is true because of the time required for examination, technical requirements, and the variety of forms of electronic media, as explained below:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing electronic data for attribution evidence and conducting a proper forensic examination requires considerable time, and taking that much time on the PREMISES could be unreasonable. Given the ever-expanding data storage capacities of computers and storage media, reviewing such evidence to identify

the items described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. The variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

27. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for would authorize seizing, imaging, or otherwise copying computers and storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

28. Because several people may share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

VI. CONCLUSION

29. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the PREMISES there exists evidence of crimes. Accordingly, a search warrant is requested.

30. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application and search warrant. I believe that sealing these documents is necessary because, given the confidential nature of this investigation, disclosure would severely jeopardize the investigation in that it might alert the target(s) of the investigation at the PREMISES to the existence of an investigation and likely lead to the destruction and concealment of evidence, and/or flight.

WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS 981 Park Place, Apt 2C, Brooklyn, NY 11213.

IT IS FURTHER REQUESTED that all papers submitted in support of this application, including the application and search warrant, be sealed until further order of the Court.

Brian Uribe
Special Agent
United States Department of Homeland Security, Homeland Security Investigations

Sworn to before me this
9th day of September, 2016

S/POHORELSKY

TH . POHORELSKY
UN TE JUDGE
EA YORK

ATTACHMENT A
Property to Be Searched

The PREMISES is located within a 6-story brick apartment building at 981 PARK PLACE, APT 2C, BROOKLYN, NY 11213. The front entrance is clearly marked as being address number "981-985" and is locked with a metal door that requires a key for entry. On July 27, 2016 HSI case agent Brian Uribe entered the building and located apartment 2C, which is located on the 2nd floor, to the left of exiting the elevator. The door to apartment 2C is described as being a dark-green metal door with a door bell button with a label on it that lists it as "2C."

ATTACHMENT B

Property to be Seized

ITEMS TO BE SEIZED FROM THE SUBJECT PREMISES, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2252 and 2252A:

1. Images of child pornography and files containing images of child pornography and records, images, information, or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A, in any form wherever they may be stored or found;

2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution, and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

   a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

   b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.

7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

8. Records evidencing occupancy or ownership of the PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Records or other items which evidence ownership or use of computer equipment found in the PREMISES, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.

11. Address books, names, lists of names and addresses of individuals believed to be minors.

12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors.

13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.

14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Computers[1] or storage media[2] that contain records or information (hereinafter "COMPUTER") used as a means to commit violations of 18 U.S.C. §§ 2252 and 2252A.

---

[1] A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including

All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, including:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

---

desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

[2] A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

i. contextual information necessary to understand the evidence described in this attachment;

16. Records and things evidencing the use of the Internet Protocol address 24.228.93.157, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. Internet Protocol addresses used by the COMPUTER;

c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

17. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A.